

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10004403 A

(43) Date of publication of application: 06.01.98

(51) Int. Cl.

H04L 9/16
G06F 12/14
G06K 17/00
H04L 9/08

(21) Application number: 08155696

(22) Date of filing: 17.06.96

(71) Applicant: N T T DATA TSUSHIN KK

(72) Inventor: KOBAYASHI TAKAFUMI
SUGANO NAOYUKI

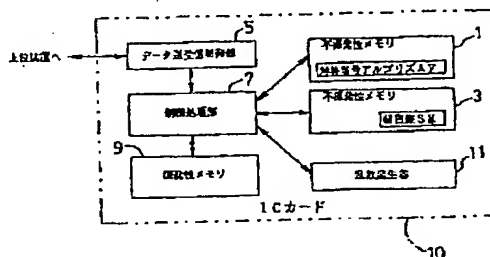
(54) ENCRYPTION DEVICE, DECODE DEVICE AND
METHOD THEREFOR

COPYRIGHT: (C)1998,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To make it hard to illegally decode a secret key by updating a temporary key as a secret key in every preprocessing or postprocessing in encryption and decode processing.

SOLUTION: A control processing part 7 reads symmetrical cipher algorithm F from 1st nonvolatile memory 1, makes the algorithm F process a secret key SK and a random number which are stored in volatile memory 9 and stores the information generated from this processed result as a key for temporary cipher processing, i.e., a temporary key in the memory 9. Next, the part 7 makes the algorithm F process a clear text and the temporary key which are stored in the memory 9 and stores this processed result as a cipher text in the memory 9. When the cipher text is created in this way, the part 7 reads the temporary key stored in the memory 9, rewrites and updates a secret key which is stored in 2nd nonvolatile memory 3 with this temporary key and prepares for the next encryption processing.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-4403

(43) 公開日 平成10年(1998) 1月6日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/16			H 0 4 L 9/00	6 4 3
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B
G 0 6 K 17/00			G 0 6 K 17/00	E
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 C

審査請求 未請求 請求項の数 7 O L (全 10 頁)

(21) 出願番号 特願平8-155696

(22) 出願日 平成8年(1996) 6月17日

(71) 出願人 000102728

エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目3番3号

(72) 発明者 小林 孝文

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

(72) 発明者 菅野 直行

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

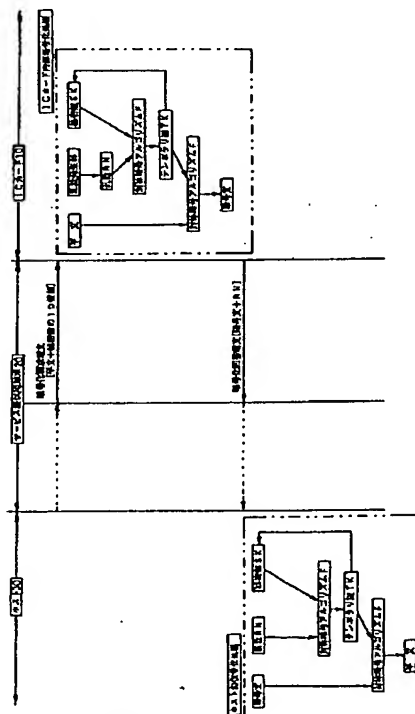
(74) 代理人 弁理士 三好 秀和 (外1名)

(54) 【発明の名称】 暗号化装置、復号化装置およびその方法

(57) 【要約】

【課題】 暗号化処理または復号化処理の都度、秘密鍵を更新し、秘密鍵の不正な解読を困難にした暗号化装置、復号化装置およびその方法を提供する。

【解決手段】 乱数RNおよび秘密鍵SKを対称暗号アルゴリズムFにより処理してテンポラリ鍵TKを生成し、該テンポラリ鍵TKおよび平文または暗号文を対称暗号アルゴリズムにより処理して暗号文または平文を生成するとともに、秘密鍵SKをテンポラリ鍵TKで更新し、次の暗号化処理または復号化処理に備えている。



【特許請求の範囲】

【請求項1】 秘密鍵および乱数を対称暗号アルゴリズムにより処理して一時鍵を生成し、この一時鍵および暗号化すべき明文または復号化すべき暗号文を当該対称暗号アルゴリズムによって処理して暗号文または明文を生成する方法であって、前記一時鍵を暗号化処理および復号化処理における処理前または処理後に、その都度、秘密鍵として更新することを特徴とする暗号化復号化方法。

【請求項2】 暗号化すべき明文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、乱数を発生する乱数発生手段と、暗号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数発生手段からの乱数および前記秘密鍵を処理し、暗号処理用の一時鍵を生成する一時鍵生成手段と、前記明文および前記一時鍵を前記対称暗号アルゴリズムによって処理し、暗号文を生成する暗号文生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを特徴とする暗号化装置。

【請求項3】 復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、復号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数および秘密鍵格納手段に格納されている秘密鍵を処理し、復号処理用の一時鍵を生成する一時鍵生成手段と、前記暗号文および前記一時鍵を前記対称暗号アルゴリズムによって処理し、明文を生成する明文生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを特徴とする復号化装置。

【請求項4】 暗号化すべき明文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、乱数を発生する乱数発生手段と、暗号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、

前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記明文および前記秘密鍵を処理し、暗号文を生成する暗号生成手段と、

前記対称暗号アルゴリズムにより前記乱数発生手段からの乱数および前記秘密鍵を処理し、一時鍵を生成する一時鍵生成手段と、

前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを特徴とする暗号化装置。

【請求項5】 復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、復号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記暗号文および秘密鍵格納手段に格納されている秘密鍵を処理し、明文を生成する明文生成手段と、前記乱数および前記秘密鍵を前記対称暗号アルゴリズムによって処理し、一時鍵を生成する一時鍵生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを特徴とする復号化装置。

【請求項6】 暗号化すべき明文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、乱数を発生する乱数発生手段と、暗号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数発生手段からの乱数および前記秘密鍵を処理し、一時鍵を生成する一時鍵生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段と、前記明文および前記更新手段で更新された秘密鍵を前記対称暗号アルゴリズムによって処理し、暗号文を生成する暗号文生成手段とを有することを特徴とする暗号化装置。

【請求項7】 復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、復号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数および秘密鍵格納手段に格納されている

秘密鍵を処理し、復号処理用の一時鍵を生成する一時鍵生成手段と、

前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段と、

前記平文および前記更新手段を更新された秘密鍵を前記対称暗号アルゴリズムによって処理し、平文を生成する平文生成手段とを有することを特徴とする復号化装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば IC カード内で対称暗号アルゴリズムと秘密鍵を用いて行われる暗号化処理または復号化処理において秘密鍵の不正な解読を困難にすべく暗号化処理または復号化処理の都度秘密鍵を更新する暗号化装置、復号化装置およびその方法に関する。

【0002】

【従来の技術】システム内で扱うデータの機密性を高めるために、例えば IC カードを用いてデータの暗号化処理を行う場合、比較的短い時間で暗号化処理が可能であるとともに、解読が比較的困難とされている対称暗号アルゴリズムおよび秘密鍵を IC カード内に格納しておき、IC カード内でデータの暗号化処理を行う方式が有力視されている。

【0003】このように、IC カード内で対称暗号アルゴリズムと秘密鍵を用いて暗号化処理を行う方式においても、最近のコンピュータ技術および暗号解読技術の進歩により、暗号文とこの暗号文の元となった生データである平文のペアをいくつか取得することにより、IC カード内に格納されている秘密鍵を外部ハッカー等により解読できる可能性があることが発表されている。

【0004】このような外部ハッカー等による秘密鍵の不正な解読をより困難にするために、対称暗号アルゴリズムをより複雑にしたり、または IC カード内に格納された秘密鍵のあるタイミングにより、または暗号化処理を行う度に、システム側で新しい秘密鍵を生成して IC カードに送信し、今まで使用されていた IC カード内の秘密鍵を新しい秘密鍵で更新することが考えられている。

【0005】

【発明が解決しようとする課題】上述したように、例えば IC カード内で対称暗号アルゴリズムおよび秘密鍵を用いて暗号化処理を行う方式において、外部ハッカー等による秘密鍵の不正な解読を防止するために考えられている方法のうち、対称暗号アルゴリズムをより複雑にする方法は、複雑なアルゴリズムを開発するために多くの時間とコストがかかるとともに、更に複雑なアルゴリズムの複雑性、すなわち解読困難性を評価するための時間とコストもかかるという問題に加えて、またアルゴリズムが複雑になればなるだけ、IC カード内の処理時間が増大するという問題がある。

【0006】また、システム側で新しい秘密鍵を生成し、IC カードに送信して更新する方法は、どのタイミングで、すなわちどれくらいの時間をおいてシステム側で新しい秘密鍵を生成し、IC カードに送信して更新すればよいのかを検証および保証することが困難であるという問題があるとともに、またシステム側で生成した新しい秘密鍵を IC カードに送信する際に、新しい秘密鍵を外部ハッカー等に盗まれる可能性があるが、これを防止し、安全に IC カードに送信するために、システム側で生成した新しい秘密鍵を更に別の秘密鍵で暗号化し、IC カードに送信する必要があるなどのように処理が更に複雑になるという問題がある。

【0007】本発明は、上記に鑑みてなされたもので、その目的とするところは、暗号化処理または復号化処理の都度、秘密鍵を更新し、秘密鍵の不正な解読を困難にした暗号化装置、復号化装置およびその方法を提供することにある。

【0008】

【課題を解決するための手段】上記目的を達成するため、請求項 1 記載の本発明は、秘密鍵および乱数を対称暗号アルゴリズムにより処理して一時鍵を生成し、この一時鍵および暗号化すべき平文または復号化すべき暗号文を当該対称暗号アルゴリズムによって処理して暗号文または平文を生成する方法であって、前記一時鍵を暗号化処理および復号化処理における処理前または処理後に、その都度、秘密鍵として更新することを要旨とする。

【0009】請求項 1 記載の本発明にあっては、対称暗号アルゴリズムにより一時鍵および平文または暗号文を処理して暗号文または平文を生成する暗号化処理または復号化処理の前または後において、その都度、一時鍵を秘密鍵として更新することで、システムで扱うデータの機密性を高めている。

【0010】請求項 2 記載の本発明は、暗号化すべき平文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、乱数を発生する乱数発生手段と、暗号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数発生手段からの乱数および前記秘密鍵を処理し、暗号処理用の一時鍵を生成する一時鍵生成手段と、前記平文および前記一時鍵を前記対称暗号アルゴリズムによって処理し、暗号文を生成する暗号文生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを要旨とする。

【0011】請求項 2 記載の本発明にあっては、対称暗号アルゴリズムにより乱数発生手段からの乱数および秘

密鍵を処理して一時鍵を生成し、該一時鍵および平文を対称暗号アルゴリズムにより処理して暗号文を生成するとともに、秘密鍵格納手段に格納されている秘密鍵を一時鍵で更新し、次の暗号化処理に備えている。

【0012】請求項3記載の本発明は、復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、復号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数および秘密鍵格納手段に格納されている秘密鍵を処理し、復号処理用の一時鍵を生成する一時鍵生成手段と、前記暗号文および前記一時鍵を前記対称暗号アルゴリズムによって処理し、平文を生成する平文生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを要旨とする。

【0013】請求項3記載の本発明にあっては、対称暗号アルゴリズムにより暗号文の生成に用いられた秘密鍵乱数および暗号文の生成に用いられた乱数を処理して一時鍵を生成し、該一時鍵および暗号文を対称暗号アルゴリズムにより処理して平文を生成するとともに、秘密鍵格納手段に格納されている秘密鍵を一時鍵で更新し、次の復号化処理に備えている。

【0014】また、請求項4記載の本発明は、暗号化すべき平文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、乱数を発生する乱数発生手段と、暗号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記平文および前記秘密鍵を処理し、暗号文を生成する暗号生成手段と、前記対称暗号アルゴリズムにより前記乱数発生手段からの乱数および前記秘密鍵を処理し、一時鍵を生成する一時鍵生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを要旨とする。

【0015】請求項4記載の本発明にあっては、対称暗号アルゴリズムにより平文および秘密鍵を処理して暗号文を生成するとともに、対称暗号アルゴリズムにより乱数および秘密鍵を処理して一時鍵を生成し、秘密鍵格納手段に格納されている秘密鍵を該一時鍵で更新し、次の暗号化処理に備えている。

【0016】請求項5記載の本発明は、復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、復号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、対称暗号アルゴリズム

格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記暗号文および秘密鍵格納手段に格納されている秘密鍵を処理し、平文を生成する平文生成手段と、前記乱数および前記秘密鍵を前記対称暗号アルゴリズムによって処理し、一時鍵を生成する一時鍵生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段とを有することを要旨とする。

【0017】請求項5記載の本発明にあっては、対称暗号アルゴリズムにより暗号文および秘密鍵を処理して平文を生成するとともに、対称暗号アルゴリズムにより暗号文の生成に用いられた秘密鍵乱数および暗号文の生成に用いられた乱数を処理して一時鍵を生成し、秘密鍵格納手段に格納されている秘密鍵を該一時鍵で更新し、次の復号化処理に備えている。

【0018】更に、請求項6記載の本発明は、暗号化すべき平文および暗号処理用の秘密鍵の識別情報を受信する受信手段と、乱数を発生する乱数発生手段と、暗号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、前記識別情報により前記秘密鍵格納手段から前記秘密鍵を検索する秘密鍵検索手段と、前記対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数発生手段からの乱数および前記秘密鍵を処理し、一時鍵を生成する一時鍵生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段と、前記平文および前記更新手段で更新された秘密鍵を前記対称暗号アルゴリズムによって処理し、暗号文を生成する暗号文生成手段とを有することを要旨とする。

【0019】請求項6記載の本発明にあっては、対称暗号アルゴリズムによって乱数および秘密鍵を処理して一時鍵を生成し、この一時鍵で秘密鍵を更新するとともに、この更新された秘密鍵および平文を対称暗号アルゴリズムによって処理して暗号文を生成している。

【0020】請求項7記載の本発明は、復号化すべき暗号文およびこの暗号文の生成に用いられた乱数を受信する受信手段と、復号処理用の秘密鍵を格納している秘密鍵格納手段と、対称暗号アルゴリズムを格納している対称暗号アルゴリズム格納手段と、対称暗号アルゴリズム格納手段に格納されている対称暗号アルゴリズムを読み出し、該対称暗号アルゴリズムによって前記乱数および秘密鍵格納手段に格納されている秘密鍵を処理し、復号処理用の一時鍵を生成する一時鍵生成手段と、前記秘密鍵格納手段に格納されている秘密鍵を前記一時鍵で更新する更新手段と、前記平文および前記更新手段を更新された秘密鍵を前記対称暗号アルゴリズムによって処理し、平文を生成する平文生成手段とを有することを要旨とする。

【0021】請求項7記載の本発明にあつては、対称暗号アルゴリズムによって暗号文の生成に用いられた秘密鍵乱数および暗号文の生成に用いられた乱数を処理して一時鍵を生成し、この一時鍵で秘密鍵を更新するとともに、この更新された秘密鍵および暗号文を対称暗号アルゴリズムによって処理して平文を生成している。

【0022】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【0023】図1は、本発明の一実施形態に係わる暗号化復号化方法を実施するICカードの構成を示すブロック図である。同図に示すICカード10は、対称暗号アルゴリズムおよび秘密鍵を用いて、外部の上位装置から送信される平文または暗号文をそれぞれ暗号化または復号化するものであり、対称暗号アルゴリズムおよび秘密鍵をそれぞれ格納している第1の不揮発性メモリ1および第2の不揮発性メモリ3を有する。また、ICカード10は、上位装置とデータの送受信を行うデータ送受信制御部5、ICカード全体の動作を制御する制御処理部7、上位装置から受信した平文、秘密鍵のID情報、ICカード10の内部で生成した暗号文や一時データ等を記憶する揮発性メモリ9、および乱数を発生する乱数発生器11を有する。

【0024】次に、図2を参照して、ICカード10で平文を暗号化する場合の処理について説明する。図1のICカード10は、図2に示すように外部の上位装置としてサービス提供用端末20を介してホスト30に接続され、該ホスト30からサービス提供用端末20を介して送信される暗号化すべき平文および秘密鍵のID情報を暗号化要求電文とともにデータ送受信制御部5で受信する。

【0025】データ送受信制御部5で受信された暗号化要求電文は、制御処理部7に供給されて解析される。制御処理部7は、受信した要求電文が暗号化要求電文であることを識別すると、該暗号化要求電文とともに送信されてきた平文およびID情報を揮発性メモリ9に格納する。ID情報は、ICカード10の第2の不揮発性メモリ3に格納されている暗号処理用の秘密鍵が第2の不揮発性メモリ3のどこに格納されているかを示す格納場所情報であり、該ID情報は第2の不揮発性メモリ3のアドレス情報でもよい。

【0026】制御処理部7は、揮発性メモリ9に格納した秘密鍵のID情報に基づいて第2の不揮発性メモリ3内を検索し、暗号処理用の秘密鍵（以下、秘密鍵SKとも称する）を第2の不揮発性メモリ3から読み出し、揮発性メモリ9に格納する。なお、このとき、第2の不揮発性メモリ3内の秘密鍵SK自体の消去は行わない。

【0027】また、乱数発生器11から乱数RNを発生させ、この発生した乱数RNを揮発性メモリ9に格納する。

【0028】それから、制御処理部7は、第1の不揮発性メモリ1から対称暗号アルゴリズムFを読み出し、揮発性メモリ9に格納した秘密鍵SKおよび乱数RNを対称暗号アルゴリズムFによって処理させ、この処理の結果生成された情報TKを一時的な暗号処理用の鍵、すなわち一時鍵TKまたはテンポラリ鍵TKとして揮発性メモリ9に格納する。

【0029】次に、制御処理部7は、揮発性メモリ9に格納しておいた平文およびテンポラリ鍵TKを対称暗号アルゴリズムFにより処理させ、この処理結果を暗号文として揮発性メモリ9に格納する。

【0030】このようにして暗号文が生成されると、制御処理部7は揮発性メモリ9に格納しておいたテンポラリ鍵TKを読み出し、このテンポラリ鍵TKで第2の不揮発性メモリ3に格納されている秘密鍵SKを書き換えて更新し、次の暗号化処理に備える。

【0031】また、制御処理部7は、揮発性メモリ9に格納した暗号文および乱数RNを暗号化回答電文とともにサービス提供用端末20を介してホスト30に返送する。

【0032】なお、図2には、ホスト30における復号化処理が示されているが、この復号化処理では、ICカード10から返送された乱数RNを用いてホスト30内に記憶されている秘密鍵SKを対称暗号アルゴリズムFにより処理して、ICカード10において暗号化のために用いられたのと同じテンポラリ鍵TKを生成し、このテンポラリ鍵TKとICカード10からの暗号文を対称暗号アルゴリズムFにより処理して平文に復号化している。また、秘密鍵SKをテンポラリ鍵TKで更新している。

【0033】次に、図3を参照して、ICカード10で暗号文を復号化する場合の処理について説明する。ICカード10は、ホスト30からサービス提供用端末20を介して復号化要求電文とともに暗号文、秘密鍵のID情報、および乱数RNを受信すると、ICカード10の制御処理部7は、受信信号を解析して、復号化要求電文であることを識別すると、暗号文、秘密鍵のID情報および乱数RNを揮発性メモリ9に格納する。

【0034】それから、揮発性メモリ9に格納したID情報で第2の不揮発性メモリ3を検索して、秘密鍵SKを第2の不揮発性メモリ3から読み出し、この秘密鍵SKおよびホスト30から受信した乱数RNを対称暗号アルゴリズムFにより処理してホスト30において暗号化のために用いられたのと同じテンポラリ鍵TKを生成する。

【0035】次に、該テンポラリ鍵TKおよびホスト30から受信した暗号文を対称暗号アルゴリズムFにより処理し、平文を生成して揮発性メモリ9に格納する。それから、制御処理部7は揮発性メモリ9に格納しておいたテンポラリ鍵TKを読み出し、このテンポラリ鍵TK

で第2の不揮発性メモリ3に格納されている秘密鍵SKを書き換えて更新し、次の処理に備える。

【0036】また、制御処理部7は、揮発性メモリ9に格納した平文を復号化回答電文としてサービス提供用端末20を介してホスト30に返送する。

【0037】なお、図3には、ホスト30における暗号化処理が示されているが、この暗号化処理の流れは図2に示したICカード10における暗号化処理と基本的に同じである。

【0038】図4は、本発明の他の実施形態に係わる暗号化復号化方法におけるICカードの別の暗号化処理を示す図である。

【0039】上述した図2に示した実施形態における平文の暗号化処理においては対称暗号アルゴリズムFにより平文とテンポラリ鍵TKを処理して暗号文を生成していたのに対して、図4に示す本実施形態では、平文と秘密鍵SKを対称暗号アルゴリズムFにより処理して暗号文を生成している点が異なるものである。

【0040】詳細に説明すると、ICカード10はホスト30からサービス提供用端末20を介して送信される暗号化すべき平文および秘密鍵のID情報を暗号化要求電文とともにデータ送受信制御部5で受信すると、暗号化要求電文が制御処理部7で解析され、平文およびID情報が揮発性メモリ9に格納される。

【0041】制御処理部7は、揮発性メモリ9に格納した秘密鍵のID情報に基づいて第2の不揮発性メモリ3内を検索し、秘密鍵SKを第2の不揮発性メモリ3から読み出し、揮発性メモリ9に格納する。

【0042】次に、制御処理部7は、第1の不揮発性メモリ1から対称暗号アルゴリズムFを読み出し、揮発性メモリ9に格納しておいた平文および秘密鍵SKを対称暗号アルゴリズムFにより処理させ、この処理結果を暗号文として揮発性メモリ9に格納する。

【0043】また、乱数発生器11から乱数RNを発生させ、この発生した乱数RNを揮発性メモリ9に格納する。

【0044】それから、制御処理部7は、第1の不揮発性メモリ1から読み出した対称暗号アルゴリズムFにより揮発性メモリ9に格納した秘密鍵SKおよび乱数RNを処理させ、一時鍵TKであるテンポラリ鍵TKを生成し、このテンポラリ鍵TKで第2の不揮発性メモリ3に格納されている秘密鍵SKを書き換えて更新し、次の暗号化処理に備える。

【0045】また、制御処理部7は、揮発性メモリ9に格納した暗号文および乱数RNを暗号化回答電文とともにサービス提供用端末20を介してホスト30に返送する。

【0046】上述した図4におけるICカード10における暗号化処理では、最初にICカード10の第2の不揮発性メモリ3に格納されている秘密鍵SKを用いて対

称暗号アルゴリズムFにより平文を処理して暗号化することを最初に行い、この後に該秘密鍵SKを更新するように説明したが、この代わりに第2の不揮発性メモリ3に格納されている秘密鍵SKを最初に更新し、この更新した秘密鍵SKを用いて対称暗号アルゴリズムFにより平文を処理して暗号化することも可能である。

【0047】具体的には、ICカード10はホスト30からサービス提供用端末20を介して平文と秘密鍵のID情報を受信すると、このID情報で第2の不揮発性メモリ3から秘密鍵SKを検索し、それから乱数発生器11から乱数RNを発生し、この乱数RNと検索した秘密鍵SKを対称暗号アルゴリズムFにより処理してテンポラリ鍵TKを生成し、このテンポラリ鍵TKで第2の不揮発性メモリ3内の秘密鍵SKを書き換えて更新する。

【0048】それから、この更新した秘密鍵SKを用いて対称暗号アルゴリズムFにより平文を処理して暗号文を生成する。そして、制御処理部7は、この暗号文および乱数RNを暗号化回答電文とともにサービス提供用端末20を介してホスト30に返送する。

【0049】なお、図4にも、ホスト30における復号化処理が示されているが、この復号化処理は図2に示したホスト30における復号化処理においてテンポラリ鍵TKの代わりに秘密鍵SKを用いた点が異なるものである。

【0050】

【発明の効果】以上説明したように、本発明によれば、システムで扱うデータの機密性を飛躍的に高めることができる上に、従来のように対称暗号アルゴリズムを複雑なアルゴリズムに変更したり、またはシステム側で秘密鍵を更新し、この更新した秘密鍵を更に別の秘密鍵で暗号化して送信するなどの複雑な処理を必要としないため、簡単かつ経済的にデータの機密性を向上することができ、外部ハッカーなどによる秘密鍵の不正な解読を適確に防止することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係わる暗号化復号化方法を実施するICカードの構成を示すブロック図である。

【図2】図1に示すICカードによる暗号化処理を示す図である。

【図3】図1に示すICカードによる復号化処理を示す図である。

【図4】本発明の他の実施形態に係わる暗号化復号化方法を示す図であり、図1に示すICカードの別の暗号化処理を示す図である。

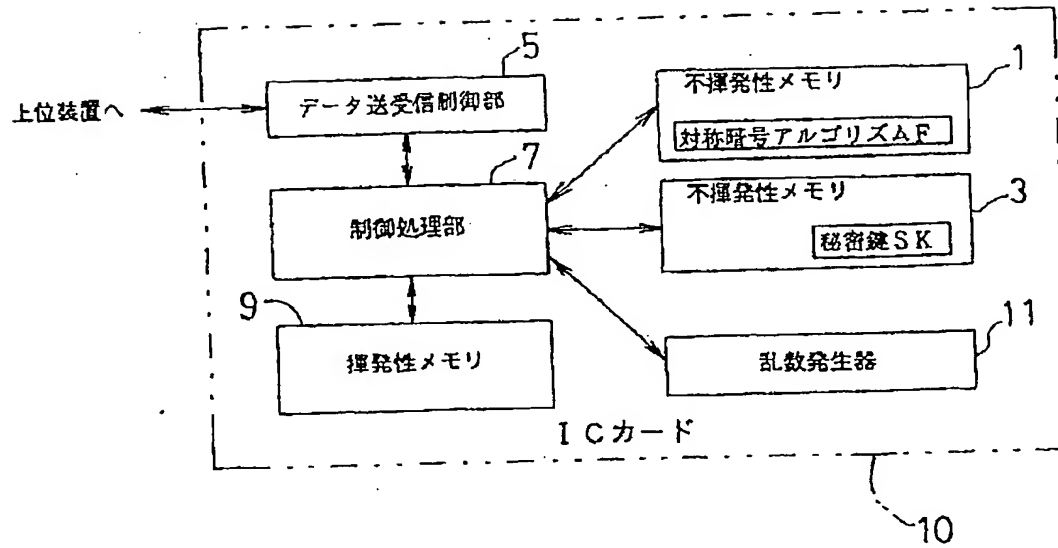
【符号の説明】

- 1 第1の不揮発性メモリ
- 3 第2の不揮発性メモリ
- 5 データ送受信制御部
- 7 制御処理部
- 9 揮発性メモリ

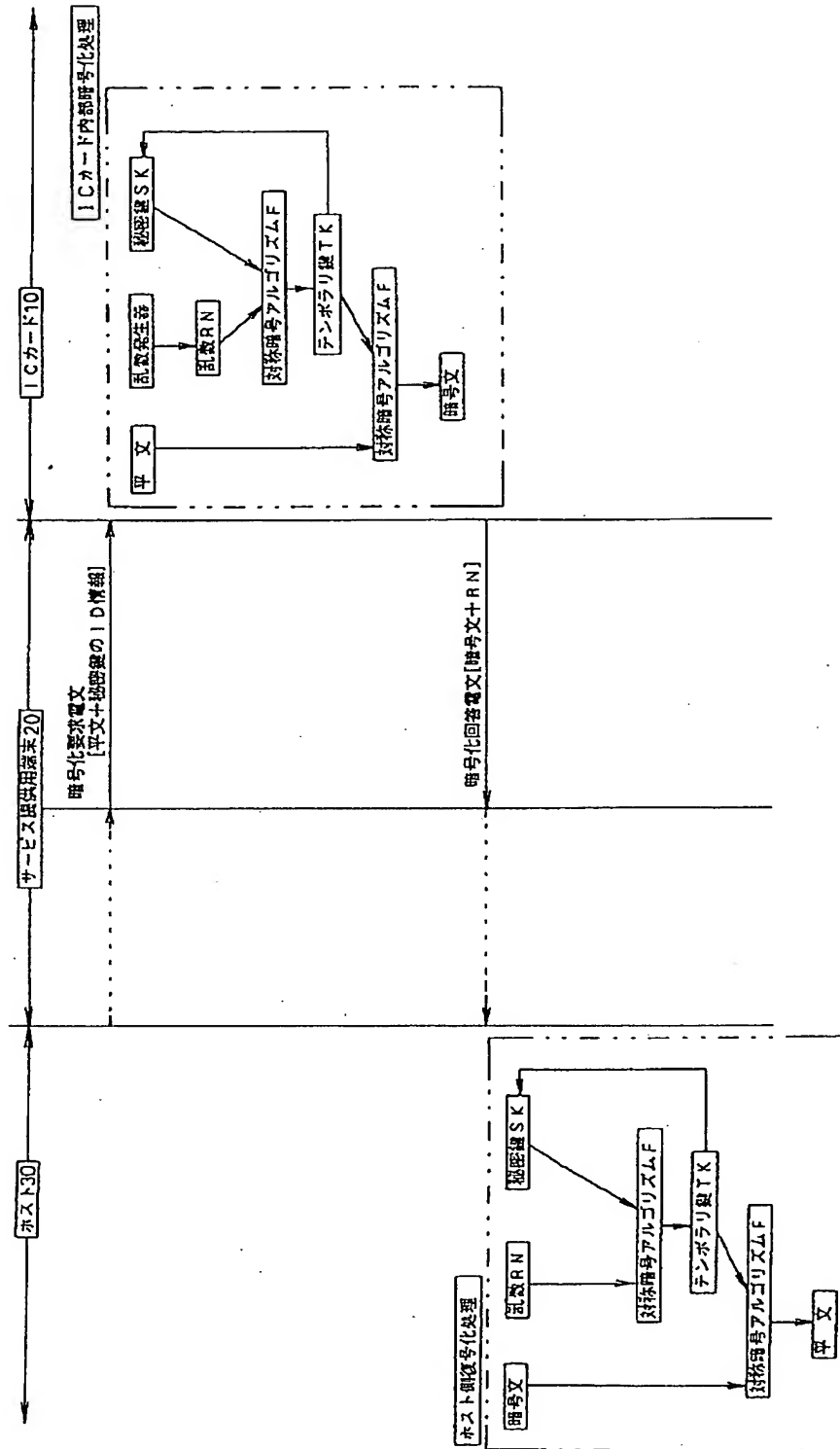
10 ICカード
11 乱数発生器

20 サービス提供用端末
30 ホスト

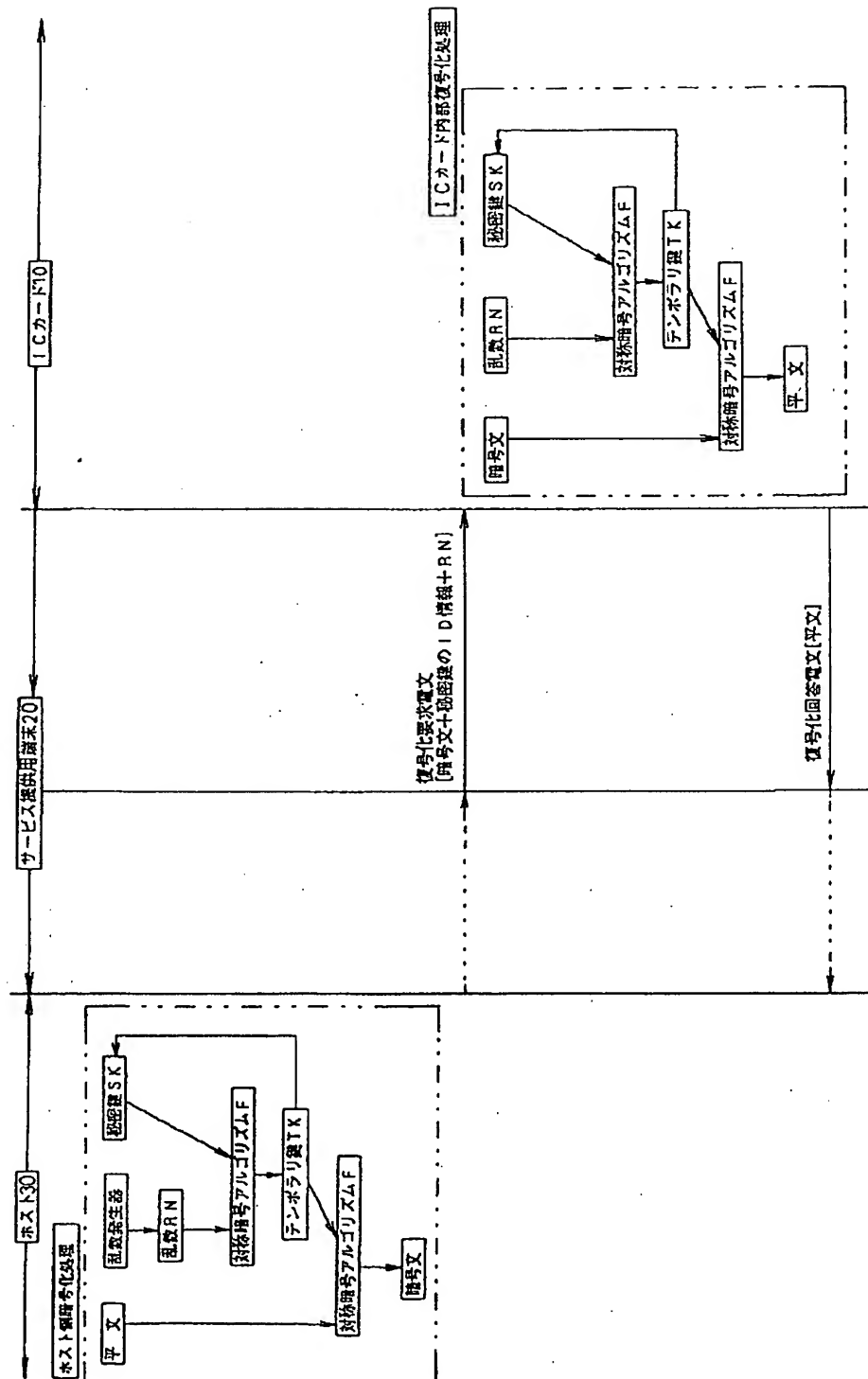
【図1】



【図 2】



【図3】



【図4】

